Zahlentheorie – Teil 2
Restklassen

ruhl

ZAHLENTHEORIE – TEIL 2 RESTKLASSEN

INHALT

GRUNDLAGEN

Die Zahlentheorie ist ein Teilgebiet der Mathematik, das sich mit den Eigenschaften der **ganzen Zahlen** beschäftigt.

$Z=\{0,\pm 1,\pm 2,\pm 3,\ldots\}$

$N=\{0,1,2,3,\ldots\}$

$Z^{+¿}=N^{+¿=\{1,2,3,\ldots\}¿}$, analog $Z^{-¿¿}$

$Z_0^{+¿}=N=\{0,1,2,3,\ldots\}¿$, analog $Z_0^{-¿¿}$

¿ und $(N,\cdot)$ sind nur kommutative Halbgruppen.

¿ ist eine kommutative Gruppe

$(Z,\cdot)$ ist eine kommutative Halbgruppe

$(Z,+,\cdot)$ ist ein kommutativer Ring mit Einselement. Das einzige, was fehlt: es gibt im Allgemeinen keine multiplikativen Inversen (d.h. die Division funktioniert nicht uneingeschränkt).

KONGRUENZEN UND RESTKLASSEN

Herr Faber hat sich heute Abend mit einem Freund auf ein Bier verabredet. Sie wollen sich um 17 677 532 Uhr vor dem Lokal treffen. …

Bei der Uhrzeit sind wir gewöhnt, für jeden Tag die Stunden neu zu zählen. 17 677 532 Uhr entspricht dann 20 Uhr, und zwar am 7. August 2017. Man sagt, die beiden Uhrzeiten sind zueinander kongruent bezüglich der Zahl 24.

$$17\,677\,532 \equiv 20 \,(mod\, 24)$$

Weitere Zeiten, die zu 20 Uhr kongruent sind: 20, 44, 68, 92, … , aber auch -4, -28, -52, …

Die Zahl 24 wird als **Modulus** bezeichnet.

Beispiel: Sie kommt um 15 Uhr und bleibt 50 Stunden. Wie spät ist es bei ihrer Abreise?

Lösung: $15+50=65=2\cdot 24+17 \equiv 17 \,(mod\, 24)$

Man sieht, zwei Zahlen sind kongruent modulo m, wenn bei beiden Zahlen nach der Division mit Rest der gleiche Rest entsteht.

Definition: Seien $m \in N^{+¿(m>0)¿}$ und $a, b \in Z$. Man sagt a ist kongruent zu b modulo m, wenn es eine Zahl $k \in Z$ gibt, sodass $a = k \cdot m + b$. In diesem Fall schreibt man $a \equiv b \,(\mathrm{mod}\, m)$.

Satz: Seien $m \in N^{+¿¿}$ und $a, b \in Z$.

$a \equiv b \,(\mathrm{mod}\, m) \quad m \vee (a-b)$

Beweis: …

Beispiel: $27 \equiv 197 \,(mod\, 10) \quad 10 \vee (27-197) \quad 10 \vee (-170)$

Zusammengefast kann man die Kongruenz auf zwei Arten definieren:

$a \equiv b \,(\mathrm{mod}\, m) \quad \exists\, k \in Z : a = k \cdot m + b \quad m \vee (a-b)$

RECHENREGELN

Satz: Sei $m \in N^{+¿¿}$ ein Modulus und $a, b, c, d \in Z$, dann gilt jeweils modulo m:

$$a \equiv b \wedge c \equiv d \Rightarrow \begin{cases} a+c \equiv b+d \\ a \cdot c \equiv b \cdot d \end{cases} \text{somit auch } n \cdot a \equiv n \cdot b \text{ und } a^n \equiv b^n \;\forall\; n \in N$$

Beweis: …

RESTKLASSEN

Satz: Die Kongruenzrelation ist eine sogenannte Äquivalenzrelation, weil sie folgende Eigenschaften besitzt:

Reflexivität: $a \equiv a \pmod m \forall\ a \in Z$

Symmetrie: $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m \forall\ a, b \in Z$

Transitivität: $a \equiv b \pmod m \wedge\ b \equiv c \pmod m \Rightarrow a \equiv c \pmod m \forall\ a, b, c \in Z$

Beweis: …

Durch die Kongruenzrelation entstehen **Äquivalenzklassen**, in welchen jeweils die Zahlen liegen, die bei Division durch den Modulus m den gleichen Rest aufweisen. Man spricht von **Restklassen**.

Beispiele für modulo 24:

$0 + 24 \cdot Z = \acute{0} = \{\ldots, -24, 0, 24, 48, 72, \ldots\}\ 1 + 24 \cdot Z = \acute{1} = \{\ldots, -23, 1, 25, 49, 73, \ldots\} \ldots$

$23 + 24 \cdot Z = \acute{23} = \{\ldots, -1, 23, 47, 71, 95, \ldots\}$

Die Elemente der Restklassen sind deren Repräsentanten. Die meistens verwendeten Repräsentanten sind $0, 1, 2, \ldots, m-1$.

Definition: Die Menge aller Restklassen modulo m wird mit Z_m bezeichnet.

$Z_m = \{\acute{0}, \acute{1}, \acute{2}, \ldots, \acute{m-1}\}$

Definition: Die Verknüpfungen

$\oplus$ mit $\acute{a} \oplus \acute{b} := \acute{a+b}$ und

$\odot$ mit $\acute{a} \odot \acute{b} := \acute{a \cdot b}$

definieren eine Restklassenaddition bzw. Restklassenmultiplikation.

Beispiel:

$\acute{13} \quad \acute{15} = \acute{13+15} = \acute{28} = \acute{4} \pmod{24}$

oder über die Repräsentanten modulo 24: $13 + 15 \equiv 28 \equiv 4 \pmod{24}$

Beispiele: $(Z_4, \oplus)$ und Verknüpfungstabelle – Kommutativgesetz, Inverse
$(Z_4, \odot)$ und Verknüpfungstabelle – Kommutativgesetz, Inverse
$(Z_5, \odot)$ und Verknüpfungstabelle – Kommutativgesetz, Inverse

Satz: $(Z_m, \oplus, \odot)$ ist ein kommutativer Ring mit Einselement. Er heißt Restklassenring modulo m.

Bemerkung: In $(Z_m, \oplus, \odot)$ bzw. in der Modulorechnung gibt es im Allgemeinen keine multiplikativ Inverse. Eine Multiplikation kann somit nicht immer zurückgerechnet werden. Es gibt nicht so etwas wie eine Division!

Beweis: … z.B. $(Z_m, \oplus)$ ist eine kommutative Gruppe. …

Schreibweise:
Es hat sich eingebürgert, statt einer Restklasse gleich nur ihren wesentlichsten Repräsentanten zu schreiben.

Als Beispiel:

$Z_6 = \{0, 1, 2, 3, 4, 5\} = \{\acute{0}, \acute{1}, \acute{2}, \acute{3}, \acute{4}, \acute{5}\}$ Statt $\acute{4} \in Z_6$ schreibt man des Öfteren $4 \in Z_6$.

$(Z_m, \odot)$ UND DIE MULTIPLIKATIV INVERSE

In $(Z_4, \odot)$ haben einige Elemente keine multiplikativ Inverse. In $(Z_5, \odot)$ haben alle Elemente eine multiplikativ Inverse. Damit ist $(Z_5, \oplus, \odot)$ sogar ein Körper. In ihm kann man, was die Addition und Multiplikation betrifft, die gleichen Rechengesetze anwenden wie in R.

Unter welchen Bedingungen hat $Z_m \setminus \{0\}$ stets multiplikativ Inverse? Die Null hat ohnehin nie eine Inverse, wir schließen sie also von vornherein aus. (Man ist das ohnehin auch von Q und R gewöhnt. Die Null hat dort ebenfalls keine multiplikativ Inverse.☺)

z.B. Z_4

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Für eine Inverse muss gelten: $a \cdot a^{\setminus} \equiv 1$

Die 1 hat eine Inverse in $Z_4 \setminus \{0\}$: $1 \cdot 1 \equiv 1$
Die 3 hat eine Inverse in $Z_4 \setminus \{0\}$: $3 \cdot 3 \equiv 1$
Die 2 hat keine Inverse in $Z_4 \setminus \{0\}$: $2 \cdot a^{\setminus} \not\equiv 1$

Satz: Ein Element $a \in Z_m \setminus \{0\}$ hat genau dann eine multiplikative Inverse, wenn a zum Modulus m teilerfremd ist, wenn also gilt
$ggT(a, m) = 1$

In $Z_4 \setminus \{0\}$ sind die Elemente $a = 1$ und 3 teilerfremd zum Modulus 4. Das Element $a = 2$ ist als gerade Zahl nicht teilerfremd zum Modulus 4 ($ggT(2,4) = 2 \neq 1$), was ihm zum Verhängnis wurde. ☺

Beweis: Sei $a \in Z_m \setminus \{0\}$. Eine multiplikativ Inverse muss folgende Bedingung erfüllen:

$$a \cdot a^{\setminus} \equiv 1 (mod\, m) \Leftrightarrow \exists\, k \in Z : a \cdot a^{\setminus} - k \cdot m = 1 \; a \cdot a^{\setminus} + m \cdot (-k) = 1$$

Dies ist eine diophantische Gleichung $ax + by = c$ mit möglichen ganzzahligen Lösungen für x und y. In unserer Gleichung steht $a^{\setminus}$ für x und $-k$ für y.

$$a \cdot a^{\setminus} + m \cdot (-k) = 1 \; [a \cdot x + b \cdot y = c]$$

Eine diophantische Gleichung hat genau dann Lösungen, wenn der $ggT(a, b) \vee c$!
Da hier $c = 1$, gibt es somit genau dann Lösungen, wenn auch der $ggT(a, m) = 1$ ■

Beispiele: Welche Elemente besitzen in $(Z_{12}, \odot)$ Inverse und welche nicht?
Welche Elemente besitzen in $(Z_{11}, \odot)$ Inverse und welche nicht?
Unter welcher Bedingung hat jedes Element von $(Z_m, \odot)$ eine Inverse?

Satz: Die algebraische Struktur $(Z_p, \oplus, \odot)$ mit $p \in P$ ist ein Körper.

Potenzieren in Z_m

Es gilt ja:

$$a \equiv b (mod\, m) \Rightarrow a^n \equiv b^n (mod\, m) \; \forall \; n \in N$$

Die Umkehrung gilt nicht unbedingt: $a \equiv b(\mathrm{mod}\, m) \Leftarrow a^n \equiv b^n(\mathrm{mod}\, m) \forall\ n \in N$

Beispiel:
Sie der Modulus $m=6$. Dann gilt einerseits
$2 \equiv 8 \Rightarrow 2^2 \equiv 8^2$Andererseits gilt nicht
$2^2 \equiv 4^2 \Rightarrow nicht\, 2 \equiv 4$

Bemerkung: Rasche Berechnung von $a^n(\mathrm{mod}\, m)$ für Computer durch Zerlegung des Exponenten immer wieder in 2-er-Potenzen.

$3^{47}=3^{46}\cdot 3=(3^{23})^2\cdot 3=\left((3^{11})^2\cdot 3\right)^2\cdot 3=\left(\left((3^5)^2\cdot 3\right)^2\cdot 3\right)^2\cdot 3=\left(\left(\left((3^2)^2\cdot 3\right)^2\cdot 3\right)^2\cdot 3\right)^2\cdot 3$Im Fall einer Modulorechnung können alle Zwischenergebnisse $\mathrm{mod}\, m$ gerechnet werden, wodurch keine großen Zahlen entstehen.

DIE EULERSCHE FUNKTION $\varphi(m)$ UND SATZ VON EULER

Sei $m \in N^{+¿¿}$ der Modulus von Z_m. Die Eulersche Funktion beurteilt nun alle natürlichen Zahlen bis m $(1 \le x \le m)$, ob sie zu m gemeinsame Teiler besitzt oder ob beide teilerfremd zueinander sind.

Beispiel: Sei $m=10$. Die betrachteten Zahlen sind $\{1, \underline{2}, 3, \underline{4}, \underline{5}, \underline{6}, 7, \underline{8}, 9, \underline{10}\}$. Dabei haben die unterstrichenen Zahlen gemeinsame Teiler mit dem Modulus $m=10$. Die fett geschriebenen Zahlen hingegen sind zu $m=10$ teilerfremd. Der Modulus $m=10$ besteht aus den Primfaktoren *2* und *5*, wohingegen die fett unterstrichenen Zahlen aus anderen Primfaktoren zusammengesetzt sind. Für sie gilt $ggT(x,m)=1$.

Die Funktion $\varphi(m)$ zählt nun alle diese teilerfremden (fettgedruckten) Zahlen.

Definition: Sei $m \in N, m>0$.
$\varphi(m)=\left|\{x \in N : 1 \le x \le m \wedge ggT(x,m)=1\}\right|$

Beispiele: $\varphi(10)=\left|\{1,3,7,9\}\right|=4$
$\varphi(18)=\left|\{1,5,7,11,13,17\}\right|=6$
$\varphi(19)=\left|\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18\}\right|=18$

Satz: Sei $m=p \in P$ eine Primzahl, dann ist $\varphi(p)=p-1$.

Beweis: … (klar! Z.B.: $m=7 \rightarrow \{1,2,3,4,5,6\}$)

Satz von Euler: Seien $m \in N, m \ge 2$ und $a \in Z$ mit $ggT(a,m)=1$,

$a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$.

Beweis:

1) *„teilerfremd × teilerfremd = teilerfremd“*
Seien $a$und b zu m teilerfremd, so besitzt m keinen Primfaktor gleich mit a und b .
$a=p_{a1}\cdot p_{a2}\cdot \ldots; b=p_{b1}\cdot p_{b2}\cdot \ldots$ und $m=q_{m1}\cdot q_{m2}\cdot \ldots$Das Produkt
$a\cdot b=p_{a1}\cdot p_{a2}\cdot \ldots \cdot p_{b1}\cdot p_{b2}\cdot \ldots$besitzt dann auch keine Primfaktoren von m .

2) Die zu m teilerfremden Zahlen $\leq m$ seien

$\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ Wir multiplizieren jedes Element dieser Menge mit einer zu m teilerfremden Zahl a

($ggT(a,m)=1$) und erhalten

$\{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(m)}\}$.

Die Menge beinhaltet wieder nur zu m teilerfremde Zahlen.

($teilerfremd \times teilerfremd = teilerfremd$ ¿

Modulo m sind das dann wieder die gleichen Zahlen, nur in anderer Reihenfolge.

z.B.: $m=9$ $\rightarrow \{1,2,3,4,5,6,7,8,9\} \rightarrow \{1,2,4,5,7,8\}$

$\{1,2,4,5,7,8\} \cdot 4 = \{4,8,7,2,1,5\} (mod\, 9)$

$\{1,2,4,5,7,8\} \cdot 14 = \{5,1,2,7,8,4\} (mod\, 9)$

Für das Produkt der Zahlen gilt

$r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv a \cdot r_1 \cdot a \cdot r_2 \cdot \ldots \cdot a \cdot r_{\varphi(m)}$ Zu m teilerfremde Zahlen $r_1, etc.$ haben multiplikativ Inverse, man kann also die Kongruenzgleichung nach $a^{\varphi(m)}$ auflösen. $r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \vee r_1^{¿} \cdot, r_2^{¿} \cdot, \ldots$

$oder\ einfacher\ r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \vee : r_1, : r_2, \ldots$

Damit folgt

$a^{\varphi(m)} \equiv 1 (mod\, m)$.

Satz (der kleine Satz von Fermat): *Für Primzahlen* $p \in P$ *gilt*

$a^{p-1} \equiv 1 (mod\, p)$

wobei $a \in Z$ kein Vielfaches von p.

Beweis: Gemäß dem Satz $\varphi(p) = p-1$ für $p \in P$ ergibt sich die Behauptung. ■
